MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDERSECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTOR, NATIONAL RECONNAISSANCE OFFICE
DIRECTORS OF THE DOD FIELD ACTIVITIES
CHIEF INFORMATION OFFICERS OF THE MILITARY DEPARTMENTS
DIRECTOR, COMMAND, CONTROL, COMMUNICATIONS AND COMPUTER SYSTEMS, JOINT STAFF
CHIEF INFORMATION OFFICERS OF THE DEFENSE AGENCIES
DIRECTOR, INTELLIGENCE COMMUNITY MANAGEMENT STAFF
INTELLIGENCE COMMUNITY CHIEF INFORMATION OFFICER
COMMANDERS OF THE UNIFIED COMBATANT COMMANDS

SUBJECT: DoD Chief Information Officer (CIO) Guidance and Policy Memorandum No. 8-8001-_____-Department of Defense and Intelligence Community GIG Overarching Policy

The Department of Defense is facing a critical challenge to unify its computing and networking capabilities to support increased levels of information assurance and interoperability. This overarching guidance and policy memorandum provides the basis for this to occur.

This attached Department of Defense and Intelligence Community GIG overarching guidance and policy is effectively immediately. It establishes policies and assigns responsibilities to further achieve effective, efficient, and economical acquisition, management, and use of all computing and networking equipment and services.

My point of contact for this effort is Mr. Terry Hagle, who can be reached at (703) 607-0235, or by email: terry.hagle@osd.pentagon.mil.

Signature Block

Guidance and Policy
For the Global Information Grid (GIG)

1 PURPOSE: This Guidance and Policy Memorandum (G&PM):

1.1 Provides overarching Department of Defense (DoD) guidance, policy and implementation direction for the Global Information Grid (GIG) as defined in enclosure (1).

1.2 Assigns management responsibilities for the GIG in compliance with Title 10, U.S.C. Armed Forces, Section 2223 (reference (a)) for IT and national security systems (NSS) throughout the DoD.

1.3 Authorizes the publication of G&PMs related to networks, enterprise computing, information assurance, interoperability, aligning the technology base, information management, and network operation.

2 APPLICABILITY and SCOPE:

2.1 This policy applies to:

2.1.1 The Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense (IG, DoD), the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components").

2.1.2 All DoD acquisitions for the GIG.

2.2 The policies and responsibilities for the Intelligence Community (IC) relating to the GIG are delineated in separate, coordinated DCI Directives (DCIDs) and IC CIO Policy Memoranda.

3 DEFINITIONS: (See Enclosure (2))

4 POLICY: It is the policy of the DoD that:

4.1 The GIG shall support DoD operations with IT and NSS solutions that offer the most effective and efficient information handling capabilities available, consistent with operational requirements and good business practices.

4.2 The DOD CIO Executive Board shall be DoD CIO's governance forum for the GIG.

4.3 The GIG shall be planned, resourced, acquired, and implemented in accordance with the DoD Information Technology Management (ITM) Strategic Plan (reference (b)).

4.4 GIG systems shall be interoperable to the extent necessary to support operational information exchange requirements.

4.5 All GIG systems shall maintain the appropriate levels of confidentiality, integrity,

availability, authentication and non-repudiation through the use of information assurance safeguards.

4.6 All DoD personnel shall be appropriately trained and, if necessary, certified to perform their designated GIG tasks.

4.7 The GIG shall include a computing and communications infrastructure to provide a full range of services for all DoD applications for all security levels.

4.8 GIG computing and communications infrastructure and services shall be provided at global, regional, local and personal levels.

4.9 All DoD applications shall be planned, designed, and implemented to use the GIG computing and communications infrastructure.

4.10 GIG plans, architectures, designs and assets shall be visible at all levels to the extent necessary for effective management and engineering.

4.11 Architecture:

4.11.1 An integrated, hierarchically based, set of architectures shall be developed and used to govern the design, implementation and evolution of the entire GIG. All GIG systems shall be planned, designed, and implemented in accordance with these architectures.

4.11.2 The current approved C4ISR Architecture Framework (reference (c)) or its successor shall be used to develop all GIG architectures. A single, integrated enterprise architecture framework, with its associated reference models, shall be developed and promulgated as an evolution of the C4ISR Architecture Framework.

4.11.3 The Joint Operational Architecture (JOA) and Joint Systems Architecture (JSA), when available, and existing Joint Technical Architecture (JTA) shall be used as the initial enterprise IT architectures. They will also form the basis for DOD's IT Architecture, as required by Clinger-Cohen Act of 1996 (reference (d)).

4.11.4 Enterprise Operational, Systems, and Technical Architectures shall be collaboratively developed and maintained to encompass the scope of the GIG and will replace the Joint Architectures as the overarching architectures for the GIG.

4.12 Requirements

4.12.1 GIG requirements shall be identified as a part of and consistent with the DoD Requirements Generation (CJSCI 3170.01A (reference (e))) process.

4.12.2 GIG requirements shall be aggregated at the appropriate level to support the efficient and effective use of resources.

4.12.3 Operational architectures, consistent with the Enterprise Operational Architecture, shall be used as the context for describing GIG requirements.

4.13 Resource Allocation.

4.13.1 GIG investment decisions shall be directly linked to DoD/IC missions, goals and outcomes in support of the warfighters, policy makers and support personnel.

4.13.2 All DoD GIG program investments shall be reviewed annually to assure required funding synchronization within and between programs.

4.14 Acquisition.

4.14.1 All DoD GIG acquisitions shall be made in compliance with DoDD 5000.1 (reference (f)) and DoD 5000.2-R (reference (g)).

4.14.2 All DoD GIG acquisitions, including upgrades or expansions of existing systems, shall comply with GIG architectures.

4.14.3 All DoD GIG programs shall be reviewed to assure synchronization and integration among programs with interdependencies (e.g., technical, infrastructure, application, or training).

4.14.4 All DoD GIG acquisition agents shall use enterprise licensing and standard contracts to the maximum extent possible.

4.15 GIG Operations Management

4.15.1 GIG service providers shall be chosen on a best value basis, unless mission requirements dictate otherwise.

4.15.2 GIG resources shall be managed to assure end-to-end information assurance, computer and network management services, and information distribution services.

4.15.3 All GIG assets shall be visible to the extent necessary to the appropriate operators for operational effectiveness and efficiency.

4.15.4 Performance metrics, as established in Service Level Agreements, shall be used to manage GIG operations and provide customer satisfaction feedback.

4.15.5 Leases, licenses and service contracts supporting the GIG shall be reviewed and revalidated at least every two years to ensure requirements still exist.

4.16 All GIG assets shall be under formal configuration management throughout their life cycle.

4.17 Any deviations from this policy shall require a waiver.

5 RESPONSIBILITIES:

5.1 DoD Chief Information Officer, in coordination with the IC CIO as appropriate, shall:

5.1.1 Chair the DoD CIO Executive Board as specified in the Charter of the DoD CIO Executive Board (reference (g)).

5.1.2 Serve as the Department of Defense Acquisition Executive for the GIG.

5.1.3 Establish vision for GIG.

5.1.4 Develop and issue the DoD ITM Strategic Plan.

5.1.5 Provide guidance for the development of GIG requirements.

5.1.6 Establish a GIG investment strategy and a process to support the implementation of GIG.

5.1.7 Establish GIG resourcing priorities based on mission requirements.

5.1.8 Establish compliance and enforcement mechanisms to achieve interoperability, information assurance, and GIG program synchronization.

5.1.9 Ensure that GIG operational effectiveness and customer satisfaction are measured and necessary corrective actions are initiated.

5.1.10 Designate GIG service providers (e.g., WANs, MANs, Regional and Global Computing).

5.1.11 Serve as the chief architect for GIG.

5.1.11.1 Co-Chair the Architecture Coordination Council. [currently as ASD(C3I)]

5.1.11.2 Establish comprehensive architecture guidance for GIG.

5.1.11.3 Ensure the development and implementation of GIG operational, systems, and technical architectures and resolve related issues.

5.1.11.4 Ensure that a process is in place to allow Components to certify that GIG acquisitions are in compliance with GIG architectures.

5.1.12 Provide for liaison and coordination with organizations external to the Enterprise regarding interfaces with the GIG (e.g. other Federal Departments and Agencies, State and Local Governments, and Allied Nations).

5.1.13 Approve or disapprove GIG waiver requests in coordination with appropriate authorities.

5.2 The OSD Principal Staff Assistants (PSAs), in addition to the responsibilities specified in paragraph 5.6, shall:

5.2.1 Coordinate with other Components, as appropriate, to maximize the use of enterprise-wide GIG capabilities and assets within their functional areas, consistent with operational requirements and best business practices.

5.2.2 Develop and maintain operational, systems, and technical architectures for their functional area consistent with the Enterprise Architectures.

5.3 The Under Secretary of Defense for Acquisition and Technology, in addition to the responsibilities specified in paragraphs 5.2 and 5.6, shall ensure, through oversight of acquisition programs and Advanced Concept Technology Demonstrations that the requirements of this Guidance and Policy Memorandum are met.

5.4 The Under Secretary of Defense, Comptroller, in addition to the responsibilities specified in paragraphs 5.2 and 5.6, shall ensure that resourcing of the GIG is consistent with the GIG investment strategies and priorities.

5.5 The Chairman of the Joint Chiefs of Staff, in addition to the responsibilities specified in paragraph 5.6, shall:

5.5.1 Ensure that Combatant Commanders identify GIG capabilities in the generation of requirements for support to Joint and Combined operations.

5.5.2 Develop Joint doctrine and associated operational procedures for the GIG.

5.5.3 Develop and maintain the Joint Operational Architecture (JOA) that describes information, information flow, and information exchanges that must occur across all information systems to support Joint Task Force (JTF) requirements.

5.6 The Heads of the DoD Components shall:

5.6.1 Comply with the policies of this Guidance and Policy Memorandum.

5.6.2 Provide necessary representation and support to the DoD CIO Executive Board.

5.6.3 Ensure that operational architectures consistent with the Enterprise Architectures are developed and maintained.

5.6.4 Ensure that GIG requirements are described in the context of operational architectures.

5.6.5 Maximize use of enterprise-wide GIG capabilities and assets consistent with operational requirements and best business practices.

5.6.6 Ensure that component-managed portions of all GIG programs are planned, resourced, acquired, and implemented in accordance with the DoD Information Technology Management (ITM) Strategic Plan and GIG resourcing priorities.

5.6.7 Ensure that GIG assets are under a formal configuration management process for their life cycle.

5.6.8 Ensure that component-managed portions of the GIG are secure, assured, and interoperable, as appropriate.

5.6.9 Ensure that all component personnel are appropriately trained and certified as necessary to perform their designated tasks associated with the GIG.

5.7 Component CIOs shall ensure that:

5.7.1 Component's ITM Strategic Plan is developed issued and consistent with the DoD ITM Strategic Plan

5.7.2 Applications are planned, designed and implemented to use the GIG computing and communications infrastructure.

5.7.3 Applications use the appropriate communications and processing services at the global, regional, local or personal level.

5.7.4 Computing and communications requirements are aggregated at the appropriate level to support the efficient and effective use of resources.

5.7.5 GIG systems and technical architectures are developed and maintained consistent with the Enterprise Architectures.

5.7.6 All GIG systems and upgrades or expansions to existing systems are built in compliance with the architectures referenced in paragraph 4.11.

5.7.7 GIG plans, architectures, systems' designs and assets are visible at all levels to the extent necessary for effective management and engineering.

5.7.8 GIG systems comply with the enterprise-wide information assurance (IA) architecture and follow operational procedures to maintain the appropriate levels of confidentiality, integrity, availability, authentication and non-repudiation.

5.7.9 GIG systems are interoperable to the extent necessary to support operational information exchange requirements.

5.7.10 GIG programs are reviewed annually to assure cross program synchronization and integration.

5.7.11 GIG programs are synchronized across the enterprise and compliant with GIG architectures prior to budget execution.

5.7.12 Enterprise licensing and standard contracts are used to the maximum extent possible.

5.7.13 GIG programs are periodically reviewed to ensure that requirements still exist for all component leases, licenses and service contracts for GIG software and services.

5.7.14 GIG operational effectiveness and customer satisfaction are measured and corrective actions are initiated, as required. Provide feedback to the DoD CIO and IC CIO upon request.

5.7.15 Disapprove or recommend approval of GIG waiver requests.

6 EFFECTIVE DATE: This Guidance and Policy Memorandum is effective immediately.

Enclosure 1: References

(a) Title X, United States Code, Section 2223.

(b) "DoD Information Technology Management (ITM) Strategic Plan," Version 1.0, March, 1997.

(c) "DoD C4ISR Architecture Framework," Version 2.0, December 18, 1997.

(d) Public Law 104-106, Clinger Cohen Act of 1996, Subdivision E, June 2, 1997.

(e) Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01A, "Requirements Generation System," August 17, 1999.

(f) DoD Directive (DoDD) 5000.1, "Defense Acquisition," March 15, 1996 with Change 1, May 21, 1999.

(g) DoD Regulation 5000.2-R, "Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs," March 23, 1998.

(h) DoD CIO Executive Board Charter.

Enclosure 2: Definitions

E2.1. Architecture: The structure of components, their relationships, and the principles and guidelines governing their design and evolution over time.

E2.2. Component Managed Portions of the GIG: That segment or portion of the GIG that is managed by a DOD Component designated as the Executive Agent, sole service provider (e.g., DISN), program manager, or other lead designator, or that is owned by a single DOD Component (base, post, camps, stations, etc. levels).

E2.3. Computing and Communications Infrastructure: Workgroup computing environments, enterprise networks, and regional and global computing environments with their related security management, infrastructure management, and information distribution services.

E2.4. Configuration Management: Includes identifying, documenting and verifying the functional and physical characteristics of an item; recording the configuration of an item; and controlling changes to an item and its documentation. It shall provide a complete audit trail of decisions and design modifications.

E2.5. Defense Acquisition Executive The individual, within the Department of Defense, charged with overall acquisition management responsibilities within his or her respective organizations. The Under Secretary of Defense (Acquisition and Technology (A&T)) is the Defense Acquisition Executive (DAE) responsible for all acquisition matters within the Department of Defense. The Department's Chief Information Officer (CIO) is the Department's Acquisition Executive for AISs and establishes acquisition policies and procedures unique to AISs.

E2.6. End to End: the inclusion of all requisite components to deliver a defined capability. For the GIG, this implies all components from the user access and display devices and sensors to the various levels of networking and processing, all associated applications, and all related transport and management services.

E2.7. Enterprise: The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and the Intelligence Community.

E2.8. Enterprise Architecture: The combination of the Enterprise Operational, Enterprise Systems, and the Enterprise Technical Architectures.

E2.9. Enterprise Computing: Comprises personal, local, regional and global computing environments

E2.10. Enterprise Networks: Comprised of all Service and Transport networks and telecommunications services, designated by the DoD CIO Executive Board as Enterprise

Networks, because they 1) provide a defined capability, 2) are available to serve multiple DoD/IC components, 3) are consistent with an established DoD/IC architecture (the Enterprise-Wide Network Architecture, or EWNA), 4) are managed with enterprise-wide oversight, and 5) provide service to any user with a validated requirement consistent with the defined capability of that service network.

E2.11. Enterprise Operational Architecture: Description of current and planned operational capability to fulfil all enterprise missions, including all operational elements and their relationships, shown in appropriate graphical models with associated textual descriptions of attributes. Operational elements include functions and tasks, information, resources (personnel and their skills, materiel, platforms and facilities), organizational units, and operational environments.

E2.12. Enterprise Systems Architecture: Description of current and planned systems capability to support the operational models described in the Enterprise Operational Architecture. It is comprised of multiple sub-views and their elements and relationships describing the different types of systems, including Sensor Systems, Weapon Systems, Information Systems, Operational Platforms, and the underlying Computing and Communication Systems that provide the information access, processing, storage, and exchange capabilities.

E2.13. Enterprise Technical Architecture: The minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements, whose purpose is to ensure that a conformant system satisfies a specified set of requirements The technical architecture view provides the technical systems-implementation guidelines upon which engineering specifications are based, common building blocks are established, and product lines are developed. The technical architecture view includes a collection of the technical standards, conventions, rules and criteria organized into profile(s) that govern system services, interfaces, and relationships for particular systems architecture views and that relate to particular operational views.

E2.14. GIG: The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all Department of Defense, National Security, and related Intelligence Community missions and functions (strategic, operational, tactical and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems.

E2.15. GIG Asset: Any Information Technology owned by the Department of Defense related to the GIG.

E2.16. GIG Operational Effectiveness: Set of performance parameters that measure the readiness of GIG assets.

E2.17. Global Computing: That portion of the regional and global computing environment that supports application processing for information that is used globally.

E2.18. Information Assurance: Information operations (IO) that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. For purposes of this definition the following meanings apply.

- ?? Availability: Timely, reliable access to data and information services for authorized users.
- ?? Integrity: Protection against unauthorized modification or destruction of information.
- ?? Authentication: Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.
- ?? Confidentiality: Assurance that information is not disclosed to unauthorized persons, processes, or devices.
- ?? Nonrepudiation: Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

E2.19. Information Management: The planning, budgeting, manipulating, controlling of information throughout its life cycle (e.g., creation or collection, processing, dissemination, use, storage, and disposition.)

E2.20. Information Technology: Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. This includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

E2.21. Intelligence Community: The departments, agencies, and activities enumerated in Sec. 3, National Security Act of 1947, as amended, (50 USC 401a), including all echelons, national through tactical.

E2.22. Interdependency: Any mutual dependence between GIG assets in DoD programs.

E2.23. Interoperability: The condition achieved when information is electronically exchanged and used to enable users to operate effectively together.

E2.24. Joint Operational Architecture: The operational architecture view of a JTF that describes the tasks and activities, the operational elements, and information flows required to accomplish or support a joint military operation.

E2.25. Joint Systems Architecture: The systems architecture view of a JTF that provides a

description, including graphics, of systems and interconnections providing for, or supporting, joint warfighting functions.

E2.26. Joint Technical Architecture: The technical architecture view that provides the DoD-wide set of rules governing the arrangement, interaction, and interdependence of system parts or elements, whose purpose is to ensure that the JTF conformant "system(s)" (as well as all other mission oriented systems) satisfies a specified set of requirements.

E2.27. Local Computing: Combination of end user devices, peripherals, local servers, local networks, user productivity tools and associated software available at a given work location, which may be fixed, mobile, or deployable.

E2.28. Metropolitan Area Network (MAN): A system of links or a ring that interconnects a relatively high concentration of LANs together within a small regional area. It is normally used as the means to efficiently connect numerous LANs to a WAN(s). The MAN also provides switching and routing between the WAN and the LANs. The demarcation points for the MAN are the service delivery nodes at the campus, post, or station router/switch and the hub/router/switch of the WAN.

E2.29. Network: An interconnection of three or more communicating entities

E2.30. Network Operations: Defined as that grouping of tasks or activities required to monitor, control, and manage the Global Information Grid.

E2.31. National Security System: any telecommunications or information system operated by the United States Government, the function, operation, or use of which—(1) involves intelligence activities; (2) involves cryptologic activities related to national security; (3) involves command and control of military forces; (4) involves equipment that is an integral part of a weapon or weapons system; or (5) subject to subsection (b), is critical to the direct fulfillment of military or intelligence missions. This does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

E2.32. Non-DoD 5000 Series Acquisitions: Other types of acquisitions, such as grants or Advanced Concept Technology Demonstrations, which are not covered by DoDD 5000.1.

E2.33. Operational Architecture: Description of the tasks and activities, operational elements, and information flows required to accomplish or support a military operation. It contains descriptions (often graphical) of the operational elements, assigned tasks and activities, and information flows required to support the warfighter. It defines the types of information exchanged, the frequency of exchange, which tasks and activities are supported by the information exchanges, and the nature of information exchanges in detail sufficient to ascertain specific interoperability requirements.

E2.34. Regional Computing: That portion of the regional and global computing environment that supports application processing for information that is applicable to a specific geographic region.

E2.35. Regional and Global Computing Environment: The combination of computing platforms, peripherals, user productivity tools and associated software that are accessed via enterprise networks and comprises regional and global computing centers.

E2.36. Service Provider: Any type of organization internal or external to DoD who has designated responsibility for the operation of one or more components of the GIG Computing and Communications Capability.

E2.37. Synchronization: Process of aligning program investments, development and implementation schedules to ensure the timely delivery of desired integrated capabilities.

E2.38. Systems Architecture: Description, including graphics, of systems and interconnections providing for, or supporting, warfighting functions. For a domain, the systems architecture view shows how multiple systems link and interoperate, and may describe the internal construction and operations of particular systems within the architecture. For the individual system, the systems architecture view includes the physical connection, location, and identification of key nodes (including materiel item nodes), circuits, networks, warfighting platforms, etc., and specifies system and component performance parameters (e.g., mean time between failure, maintainability, availability). The systems architecture view associates physical resources and their performance attributes to the operational view and its requirements per standards defined in the technical architecture.

E2.39. Technical Architecture: The minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements, whose purpose is to ensure that a conformant system satisfies a specified set of requirements The technical architecture view provides the technical systems-implementation guidelines upon which engineering specifications are based, common building blocks are established, and product lines are developed. The technical architecture view includes a collection of the technical standards, conventions, rules and criteria organized into profile(s) that govern system services, interfaces, and relationships for particular systems architecture views and that relate to particular operational views.

E2.40. Visibility: Having the awareness of the status of a resource. It may or may not involve actually monitoring the resource.

E2.41. WAN (Wide Area Network): A system of links that are used to interconnect geographic regions. The WAN normally provides routing, switching, or gateway points to MANs, LANs, or other WANs.